CLAIMS

1. An encryption/decryption device comprising:

a data structure analysis block for receiving encrypted data or data to be encrypted, analyzing the structure of the data and outputting information related to encryption as control data, the data structure analysis block also outputting the encrypted data or the data to be encrypted as processing block input data;

a data control block for outputting an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing block for performing encryption or decryption for the processing block input data according to the encryption/decryption switch signal, and outputting encrypted result or decrypted result,

wherein the shared processing block is configured to have the ability to perform encryption and decryption in either of the Cipher Block Chaining (CBC) mode and the Cipher Feedback (CFB) mode by performing Electronic Code Book (ECB) processing using input key data, and performs encryption or decryption in the mode indicated by the mode selection signal.

2. The encryption/decryption device of Claim 1, wherein the data structure analysis block analyzes a header of the encrypted data to draw out a Media Access Control (MAC) structure from the encrypted data based on information in the header, and if an extension header exists in the MAC structure and the extension header indicates that the encrypted data has been encrypted, the data structure analysis block outputs information related to encryption included in the extension header as the control data, and also removes the

extension header from the MAC structure data and outputs the result as the processing block input data.

3. The encryption/decryption device of Claim 1, wherein the data control block outputs a signal indicating in which mode, the CBC mode or the CFB mode, the processing block input data should be processed and in which key data length mode the data should be processed, as the mode selection signal, according to the control data.

4. The encryption/decryption device of Claim 1, wherein the shared processing block comprises:

an ECB processor for performing the ECB processing and outputting the result as cipher-processed data;

a first selector for selecting one of the processing block input data and the cipher-processed data according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data;

a delay device for delaying the processing block input data and the cipher-processed data received as inputs and outputting the delayed data;

a second selector for selecting one of the processing block input data, initial vector data, and the delayed processing block input data and the delayed cipher-processed data output from the delay device according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data;

an XOR operator for computing XOR of the output of the first selector and the output of the second selector and outputting the computed result;

a third selector for selecting one of the processing block input data, the output of the XOR operator, the delayed processing block input data and the delayed cipher-

processed data according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data;

a bit mask device for masking part of the key data as required according to the mode selection signal and outputting the result as mode-adaptive key data; and

a fourth selector for selecting one of the cipher-processed data and the output of the XOR operator according to the encryption/decryption switch signal and the mode selection signal, and outputting the selected data as the encrypted result or the decrypted result,

wherein the ECB processor performs either encryption or decryption as the ECB processing for the output of the third selector using the mode-adaptive key data according to the encryption/decryption switch signal and the mode selection signal, and outputs the result as the cipher-processed data.

5. The encryption/decryption device of Claim 4, wherein the bit mask device outputs the key data as it is if the mode selection signal indicates a 56-bit key mode, or otherwise masks unnecessary bits and outputs the resultant data, as the mode-adaptive key data.

6. The encryption/decryption device of Claim 4, wherein the first selector selects the processing block input data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, or otherwise selects the cipher-processed data, and outputs the selected data.

7. The encryption/decryption device of Claim 4, wherein the second selector selects the initial vector data at start of processing and thereafter selects the delayed cipher-processed data if the encryption/decryption switch signal indicates encryption and the

mode selection signal indicates the CBC mode, and outputs the selected data,

selects the initial vector data at start of processing and thereafter selects the processing block input data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data,

selects the initial vector data at start of processing and thereafter selects the delayed processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, and outputs the selected data, or

selects the initial vector data at start of processing and thereafter selects the processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode, and outputs the selected data.

8. The encryption/decryption device of Claim 4, wherein the third selector selects the output of the XOR operator if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data,

selects the processing block input data at start of processing and thereafter selects the delayed cipher-processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data,

selects the processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, and outputs the selected data, or

selects the processing block input data at start of processing and thereafter selects the delayed processing block input data if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode, and outputs the selected

data.

9. The encryption/decryption device of Claim 4, wherein the fourth selector selects the cipher-processed data if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CBC mode, and outputs the selected data,

selects the output of the XOR operator if the encryption/decryption switch signal indicates encryption and the mode selection signal indicates the CFB mode, and outputs the selected data, or

selects the output of the XOR operator if the encryption/decryption switch signal indicates decryption, and outputs the selected data.

10. The encryption/decryption device of Claim 4, wherein the ECB processor performs encryption if the encryption/decryption switch signal indicates encryption,

performs decryption if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CBC mode, or

performs encryption if the encryption/decryption switch signal indicates decryption and the mode selection signal indicates the CFB mode.

11. The encryption/decryption device of Claim 1, further comprising:

a first input selector for selecting encrypted data or the output of the shared processing block and outputting the selected data to the data structure analysis block;

a second input selector for selecting data to be encrypted or the output of the shared processing block and outputting the selected data to the data structure analysis block; and

an output selector for selecting a predetermined value or the output of the shared processing block and outputting the selected data,

wherein once processing in the shared processing block is performed for the encrypted data or the data to be encrypted for a predetermined number of times, the output selector selects the output of the shared processing block.

12. The encryption/decryption device of Claim 11, wherein the predetermined number of times is three times.

13. An encryption device comprising:

a data structure analysis block for receiving data to be encrypted, analyzing the structure of the data to determine control data and outputting the control data, the data structure analysis block also outputting the data to be encrypted as processing block input data;

a data control block for outputting a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing block for performing encryption for the processing block input data and outputting encrypted result,

wherein the shared processing block is configured to have the ability to perform encryption in either of the CBC mode and the CFB mode by performing ECB processing using input key data, and performs encryption in the mode indicated by the mode selection signal.

14. The encryption device of Claim 13, wherein the shared processing block comprises:

an ECB processor for performing the ECB processing and outputting the result as

cipher-processed data;

a first selector for selecting one of the processing block input data and the cipher-processed data according to the mode selection signal, and outputting the selected data;

a delay device for delaying the cipher-processed data received as an input and outputting the delayed data;

a second selector for selecting one of the processing block input data, initial vector data and the delayed cipher-processed data output from the delay device according to the mode selection signal, and outputting the selected data;

an XOR operator for computing XOR of the output of the first selector and the output of the second selector and outputting the computed result;

a third selector for selecting one of the processing block input data, the output of the XOR operator and the delayed cipher-processed data according to the mode selection signal, and outputting the selected data;

a bit mask device for masking part of the key data as required according to the mode selection signal and outputting the result as mode-adaptive key data; and

a fourth selector for selecting one of the cipher-processed data and the output of the XOR operator according to the mode selection signal, and outputting the selected data as the encrypted result,

wherein the ECB processor performs encryption as the ECB processing for the output of the third selector using the mode-adaptive key data, and outputs the result as the cipher-processed data.

15. A decryption device comprising:

a data structure analysis block for receiving encrypted data, analyzing the structure of the data and outputting information related to encryption as control data, the data

structure analysis block also outputting the encrypted data as processing block input data;

a data control block for outputting a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing block for performing decryption for the processing block input data and outputting decrypted result,

wherein the shared processing block is configured to have the ability to perform decryption in either of the CBC mode and the CFB mode by performing ECB processing using input key data, and performs decryption in the mode indicated by the mode selection signal.

16. The decryption device of Claim 15, wherein the shared processing block comprises:

an ECB processor for performing the ECB processing and outputting the result as cipher-processed data;

a delay device for delaying the processing block input data received as an input and outputting the delayed data;

a second selector for selecting one of the processing block input data, initial vector data and the delayed processing block input data output from the delay device according to the mode selection signal, and outputting the selected data;

an XOR operator for computing XOR of the cipher-processed data and the output of the second selector and outputting the computed result;

a third selector for selecting one of the processing block input data and the delayed processing block input data according to the mode selection signal, and outputting the selected data; and

a bit mask device for masking part of the key data as required according to the mode selection signal and outputting the result as mode-adaptive key data,

wherein the ECB processor performs either encryption or decryption as the ECB processing for the output of the third selector using the mode-adaptive key data according to the mode selection signal, and outputs the result as the cipher-processed data.

17. A transmission/reception apparatus comprising:

a downstream PHY section for converting a received signal into data and outputting the converted data;

a downstream data processing section for separating downstream data and key data from the received data and outputting the resultant data;

a first encryption/decryption device for decrypting the downstream data using the key data and outputting the decrypted data;

a storage section for storing the decrypted downstream data;

a second encryption/decryption device for encrypting upstream data read from the storage section and outputting the encrypted data;

an upstream data processing section for adding key data used for the encryption to the encrypted upstream data and outputting the resultant data; and

an upstream PHY section for converting the data output from the upstream data processing section into a signal and transmitting the signal,

wherein both the first and second encryption/decryption devices comprise:

a data structure analysis block for receiving the downstream data including encrypted data or the upstream data including data to be encrypted, analyzing the structure of the data and outputting information related to encryption as control data, the data structure analysis block also outputting the encrypted data or the data to be encrypted as

processing block input data;

a data control block for outputting an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and a mode selection signal indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing block for performing encryption or decryption for the processing block input data according to the encryption/decryption switch signal, and outputting encrypted result or decrypted result,

wherein the shared processing block is configured to have the ability to perform encryption and decryption in either of the CBC mode and the CFB mode by performing ECB processing using input key data, and performs encryption or decryption in the mode indicated by the mode selection signal.

18. An encryption/decryption method comprising:

a data structure analysis step of analyzing the structure of encrypted data or data to be encrypted to determine information related to encryption as control data, and also determining the encrypted data or the data to be encrypted as processing block input data;

a data control step of determining an encryption/decryption switch signal indicating which one of encryption and decryption should be performed, and mode selection data indicating in which mode the processing block input data should be processed, according to the control data; and

a shared processing step of performing encryption or decryption for the processing block input data according to the encryption/decryption switch signal to determine encrypted result or decrypted result,

wherein the shared processing step includes having the ability to perform

encryption and decryption in either of the CBC mode and the CFB mode by performing ECB processing using key data, and performing encryption or decryption in the mode indicated by the mode selection data.

19. An encryption method comprising:

a data structure analysis step of analyzing the structure of data to be encrypted to determine control data, and also determining the data to be encrypted as processing block input data;

a data control step of determining mode selection data indicating in which mode the processing block input data should be processed according to the control data; and

a shared processing step of performing encryption for the processing block input data to determine encrypted result,

wherein the shared processing step includes having the ability to perform encryption in either of the CBC mode and the CFB mode by performing ECB processing using key data, and performing encryption in the mode indicated by the mode selection data.

20. A decryption method comprising:

a data structure analysis step of analyzing the structure of encrypted data to determine information related to encryption as control data, and also determining the encrypted data as processing block input data;

a data control step of determining mode selection data indicating in which mode the processing block input data should be processed according to the control data; and

a shared processing step of performing decryption for the processing block input data to determine decrypted result,

wherein the shared processing step includes having the ability to perform decryption in either of the CBC mode and the CFB mode by performing ECB processing using key data, and performing decryption in the mode indicated by the mode selection data.